REMARKS

Applicants respectfully traverse and request reconsideration.

Applicants wish to thank the Examiner for the notice that claims 5-9, 12-15, 19, 34, 35, 38, 44 and 47 would be allowable if rewritten to include the limitations from the intervening claims.

Claims 1-4, 10, 16-18, 23, 24, 27-30, 32, 33, 36, 37, 39-43 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,666,420 ("Micali"). Micali describes a system for providing simultaneous electronic transactions wherein a first set of communications is exchanged between a first and second party without participation of a trusted party to attempt completion of a transaction. If the transaction is not completed using the first set of communications then the trusted party takes action to complete the transaction. A second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party.

The Office Action cites Col. 3, line 43-Col. 4, line 40 as disclosing all the limitations of claims 1-4, 10, 18, 23, 24, 27, 30, 32, 33, 36, 37 and 40-43. The third party described in the Micali reference "does not need to take any action if a transaction occurs with the parties following certain prescribed instructions." In contrast, Applicants' claimed invention, among other things, requires and forces a mandatory communication between a second party and a third party using a unique method and structure.

Micali also describes a certified mail system that requires the first party to generate and send to the second party a data stream including ciphertext, which is a message encrypted in a recipient's key. The encrypted message is then encrypted along with recipient identifier and sender identifier using a third party public key. This package is then sent to the recipient. This is referred to as step A1 (see Col. 5, lines 46-49). Upon receiving the package from the sender, the recipient digitally signs the package and sends it back to the sender as the receipt. (Col. 5, lines 50-51). If the sender receives a properly signed receipt from the recipient, the sender then sends to the recipient the message encrypted with the recipient's key. If the recipient then receives a suitable ciphertext from the sender, the recipient decrypts the message. Otherwise the recipient sends the originally received package, which is signed by the recipient, to the post office (third party) indicating that a sender has sent it and that the recipient is passing it to the post office. Hence, if a recipient is unable to decrypt a message that is resent by the sender to the recipient then the recipient forwards a previously sent package to the post office so that the post office can decrypt the original package and send the sender a value that serves as a receipt from the recipient. The post office then sends only the encrypted message back to the recipient. Since the encrypted message was encrypted using the recipient public key, the recipient already has the necessary decryption key to decrypt the message.

As Micali summarizes, if a sender sends a message encrypted with a third party key to a recipient, and the recipient does not send the sender a receipt, or if a recipient does not access the third party, the recipient will never learn the message. Otherwise, the sender is guaranteed to get a receipt for the message either from the recipient or from the third party post office. On the other hand, upon receiving an encrypted message, the recipient is guaranteed he will understand it, either helped by the sender sending an encrypted message or by the post office sending the encrypted message. (Col. 6, lines 54-61). Hence, in the instance where the post office is used to facilitate encrypted message confirmation, the only operation that the third party performs is to affectively resend the encrypted message to the recipient while also sending a value Z signed by the recipient as a receipt to the sending application. The recipient does not receive a recovered decryption key from the post office but merely receives the encrypted message (see, for example, Col. 5, line 67).

Applicants claim a distinctly different approach. With Applicants' method and apparatus, the recipient is forced to communicate with the third party to receive a decryption key which facilitates mandatory communication between the receiving party and the third party and the receiving party then decrypts the data based on the recovered decryption key. This is done, for example, by providing a double key package by the receiving party to a third party, the third party then decrypts, in part, the double key package to recover a decryption key for the second party using a third party based decryption key. It does not appear that Micali uses the post office to send a decryption key to a recipient or to recover a decryption key for the recipient. To the contrary, Micali appears to teach simply resending the encrypted message back to the recipient if the recipient is unable to provide a receipt to the sender. The post office in Micali decrypts a package with its secret key to make sure it is a package for the sender and sends the sender a value Z, namely the package signed by the recipient as the receipt. The recipient and the encrypted message is already encrypted using the public key to the recipient as noted in step A1.

As noted in the specification, the invention uses a double key package configured in a way that requires a recipient to obtain a decryption key from a third party, as such the recipient cannot decrypt a message sent by the recipient without assistance from a third party to actually decrypt the information. In one example, an originator produces a signed message with a third party based encrypted security token to a recipient. A signed message with the third party based encrypted security token includes a double key package and accompanying ciphertext. In this example, the recipient receives the signed message with the third party based encrypted security token and generates a request to the third party to request a cryptographic key to the site for the encrypted message. As part of the request, the recipient processor passes the double key package to the third party processor and the request is logged by the third party to provide message delivery indication to the originator. The third party processor then partially decrypts the double key package received from the recipient using a third party based decryption key to recover the decryption key for the second party. By way of example, the message may be encrypted using asymmetric encryption key which then may be wrapped with the recipient public encryption key which is referred to as a security token 46. The security token 46 is then encrypted using a second symmetric key associated with the third party to produce a first key package which is an encrypted security token. The second symmetric key is encrypted using another encryption key such as a third party public key to produce a second key package. As such, in Applicants' invention a second key, such as a second symmetric key, must be obtained from the third party in order for the recipient to decrypt the message. A request is made to the third party for this key by the recipient. As such, the cited reference does not appear to teach or suggest, among other things, providing a double key package to a second party and then having the second party communicate the double key package to a third party and then partially decrypting the double key package to recover a decryption key for the second party to facilitate mandatory communication between the second party and the third party and decryption of data based on the recovered decryption key. Accordingly the claims are believed to be in condition for allowance.

The dependent claims add additional novelty and non-obvious subject matter are not taught or suggested by the cited reference.

As to claims 16, 17, 21, 22, 29 and 39, these claims require, among other things, an authorized status request that is used by a third party to generate message delivery status data. by way of example, a first party may send a request to the third party to determine whether or not a message has been delivered to a recipient. In response to this status request, the third party verifies the authorized request by verifying a digital signature sent by the sending party and determines whether that sending party should receive the message delivery status. This is different from the Micali reference.

The Office Action cites Col. 5, lines 45-67 as teaching such an operation. As a preliminary matter, Applicants respectfully reassert the relevant remarks made with respect to the independent claims. In addition, the cited portion of Micali merely indicates that the post office sends the original package originally sent by the sender that includes a signature by the recipient as received by the third party from the recipient. Applicants are unable to find where the recited portion mentions a message delivery status request being made by the sender or verifying that the requesting party is authorized to receive the message delivery status. Accordingly, these claims are believed to be allowable.

As to claims 20 and 28, Applicants respectfully reassert the relevant remarks made above with respect to the independent claims and again note that the Micali does not appear to teach or suggest signing a double key package to produce a signed message with a third party based encryption security token as claimed.

Claims 11, 25, 26 and 31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Micali in view of U.S. Patent No. 5,351,295 ("Perlman"). Perlman is directed to a secure method of neighbor discovery over a multi-access medium wherein stations in a communications network are informed of the addresses of their neighbors by means of identifying messages transmitted by the stations. For protection, passwords are encrypted with versions of the identities of the stations transmitting the messages. The encrypted passwords may also include time stamps. Perlman does not appear to be directed to a method or apparatus for providing secure communication of data using a third party as claimed. Moreover, the time stamps of

Perlman are not time stamps submitted in response to the receipt of, among other things, a double key package as claimed. Accordingly, the claims are also believed to be in condition for allowance.

Applicants respectfully reassert the relevant remarks made above with respect to the independent claims and again note that the present claims include, among other things, applying time stamped data by a third party for a sending party based on receipt of the double key package and based on a received message data. Again, there is no double key package as claimed in the Micali reference and no time stamp of that information indicating that the third party has received it. In addition, the Office Action alleges that the Micali reference teaches that the trusted party decrypts the encrypted message and sends it to the second party who decrypts the message with the public key. There is no communication of a recovered decryption key package sent to the second party to enable the decryption of the message by the second party. The message in Micali is encrypted with the second party's public key so that the second party need not obtain a decryption key from the third party. Accordingly these claims are in condition for allowance. In addition, the Perlman reference also does not teach the double key package or time stamping by a third party to a first party based on receipt of message data in a double key package received back from the second party by the third party as claimed. Accordingly these claims are also in condition for allowance.

Perlman is directed to a secure method of neighbor discovery over a multi-access medium wherein stations in a communications network are informed of the addresses of their neighbors by means of identifying messages transmitted by the stations. For protection, passwords are encrypted with versions of the identities of the stations transmitting the messages, the encrypted passwords may also include time stamps. Perlman does not appear to be directed to a method or apparatus for providing secure communication of data and applying the third party as claimed. Moreover, the time stamps are not time stamps submitted in response to the receipt of, among other things, a double key package as claimed. Accordingly, the claims are also believed to be in condition for allowance.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "Version with markings to show changes made."

Accordingly, Applicant respectfully submits that the claims are in condition for allowance and that a timely Notice of Allowance be issued in this case. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a telephone conference will advance the prosecution of this application.

Respectfully submitted,

By:________________________
Christopher J. Reckamp
Registration No. 34,414

Date: April 1, 2003

Vedder, Price, Kaufman & Kammholz
222 N. LaSalle Street
Chicago, IL 60601
PHONE: (312) 609-7500
FAX: (312) 609-5005

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In the Claims:

Please amend claims 5, 12 and 34 to read as follows:

5. (Amended) The method of claim 1 [in] including the steps of:

generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;

providing the cipher text to the second party;

encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package; and

encrypting the first key package using a third encryption key associated with the third party to [the] produce a double key package.

12. (Amended) The method of claim 10 [in] including the steps of:

generating cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;

providing the cipher text to the second party;

encrypting the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key [packaging]package; and

encrypting the first key package using a third encryption key associated with the third party to [the] produce a double key package.

34. (Amended) The storage medium of claim 32 including data representing executable instructions that cause a processing device to:

generate cipher text by encrypting data with a first cryptographic key (Ks1) by the first party;

provide the cipher text to the second party;

encrypt the cryptographic key (Ks1) using a second encryption key associated with the second party to produce a first key package; and

encrypt the first key package using a third encryption key associated with the third party to produce a double key package.